Configuration réseau d'une machine Linux

Abdelali SAIDI

abdelali.saidi@gmail.com

Plan

Plan



Les adressages IP

Présentation

- Chaque machine appartenant à un réseau doit au moins posséder une adresse IP
- Cette adresse est assignée à l'interface d'une machine
- L'adresse IPv4 est composée de 4 octets

Notation des adresses

- 212.50.14.82
- 11010100.00110010.00001110.01010010



Réseaux - Masques - Adresses réseau et de diffusion

L'adresse IP

Une adresse IP est composée de deux parties:

- Partie réseau
- Partie machine

Le masque

Le masque spécifie le nombre de bits réservé à la partie machine (en lui appliquant un ET logique avec l'adresse IP)

- 11111111.11111111.11111111.11000000 (/26)
- Cela veut dire que les 26 premiers bits de l'adresse IP forment l'adresse réseau auquel la machine appartient.



Réseaux - Masques - Adresses réseau et de diffusion

L'adresse Réseau

L'adresse réseau se spécifie en remplaçant la partie machine par des zéros

- 212.50.14.82/26 appartient au réseau 212.50.14.64/26

L'adresse de diffusion

L'adresse de diffusion se spécifie en remplaçant la partie machine par des uns

- L'adresse broadcast du réseau 212.50.14.64/26 : 212.50.14.127/26



Les classes IP

Présentation

La classe d'une adresse IP réseau détermine la taille de ce dernier. Pour déterminer de quelle classe appartient un réseau, il faut examiner ses deux premiers bits.

Les classes en IPv4

Premiers 2 bit	**Classe IP**	**Taille du réseau**	**Nombre d'adresses IP du réseau**	**Exemple**
00 ou 01	A	1 octet	224 = 16777216	115.0.0.1 **01**110011.00000000.00000000.00000001
10	B	2 octets	216 = 65536	130.1.1.1 **10**000010.00000001.00000001.00000001
11	C	3 octets	28 = 65536	212.50.14.82 **11**010100.00110010.00001110.01010010

Les adresses privées

Présentation

Dans chaque classe d'adresses IP, on trouve des réseaux réservés pour des besoins privés. Les adresses de ces réseaux sont utilisées uniquement dans des réseaux internes.

Les adresses privées

Classe IP	Adresses privées
A	10.X.X.X
B	172.16.X.X - 172.131.X.X
C	192.168.X.X



Les sous réseaux

- La division en classe IP provoque un gaspillage important d'adresses
- En utilisant des masques différents on peut subdiviser un réseau en plusieurs sous-réseaux selon le besoin

Exemple

- Segmenter le réseau 192.168.1.0/24 en 4 sous-réseau de même taille
- Faite pareil pour 4 sous-réseaux sachant que le 1er contiendra 32 machines, le 2ème et le 3ème 64 machines, le 4ème contiendra 128

La suite TCP/IP

Présentation

- On désigne par “la suite TCP/IP” l'ensemble des protocoles de base sur lesquels s'appuient toutes les communications Internet.
- En l'occurrence : IP, ICMP, UDP et TCP



La suite TCP/IP

Le modèle TCP/IP

Couche	Description	Protocoles
Application	La couche supérieure – comme son nom l'indique. On y trouve les applications réseau	FTP, HTTP, SMPT, POP, IMAP, ...
Transport	Transmission des données	TCP, UDP
Internet	Datagrammes et routage – connexion des réseaux	IP, ICMP, ARP(?), RIP, BGP, IGMP
Network Access	Communication au niveau physique	Ethernet, Token Ring, etc.

La suite TCP/IP

Protocoles

Protocole	Description
IP	C'est le protocole utilisé pour le découpage de l'information (les segments TCP ou UDP) en paquets (datagrammes) et pour le routage de ces paquets de l'émetteur au destinataire. C'est aussi le protocole qui définit l'adressage des différentes machines connectées à l'Internet et le regroupement de ces machines en réseaux.
TCP	*Transmission Control Protocol* – c'est le protocole fiable de transmission des données. Il travaille en mode connecté pour transmettre les données d'une application à une autre tout en assurant le contrôle de l'intégrité des données.
UDP	*User Datagram Protocol* – ce protocole assure aussi la transmission des données entre applications mais en mode « non fiable » : l'intégrité des données n'est pas contrôlée. Les applications utilisant ce protocole doivent elles-mêmes vérifier cette intégrité. Ce protocole est plus performant que TCP.
ICMP	*Internet Control Message Protocol* – ce protocole est destiné à gérer les informations relatives aux erreurs pouvant survenir sur le réseau.

Les ports

Présentation

- Les ports servent à distinguer entre plusieurs applications
- Les ports de 1 à 1023 sont réservés aux serveurs
- Les ports de 1024 à 65 535 sont utilisés dynamiquement
- Liste de services réseaux classiques se trouve sur /etc/services

Plan

Les fichiers de configuration

/etc/hosts

Le fichier /etc/hosts permet de résoudre les noms sans le mécanisme DNS

/etc/resolv.conf

Le fichier /etc/resolv.conf est le fichier de configuration du client DNS. On y trouve l'adresse IP des serveurs DNS ainsi que le domaine de recherche par default.

host et dig

Les commandes host et dig sont des utilitaires de recherche DNS

- host www.google.ma
- dig www.google.ma



Les fichiers de configuration

/etc/nsswitch.conf

Le fichier /etc/nsswitch.conf permet de spécifier quelle source d'information consulter pour résoudre les noms de domaine et dans quel ordre. Exemple:

- Hosts: files dns (pour la résolution des noms de machines, on commencera par chercher sur les fichiers et puis en utilisant un service dns)

/etc/sysconfig/network

Le fichier /etc/sysconfig/network contient des informations à propos de la configuration réseau d'une machine. On y spécifie:

- S'il faut démarrer automatiquement le service réseau
- Le nom de la machine
- La passerelle (GATEWAY)
- L'interface réseau (GATEWAYDEV)



Les fichiers de configuration

/etc/sysconfig/network-scripts

Le fichier /etc/sysconfig/network-scripts contient des informations spécifiques à chaque interface réseau.

```
#/etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
IPADDR=134.157.9.52
NETMASK=255.255.255.0
NETWORK=134.157.9.0
BROADCAST=134.157.9.255
ONBOOT=yes
```

Les fichiers de configuration

/etc/network/interfaces

Les machines Debian stockent les informations de toutes les interfaces réseau dans le fichier /etc/network/interfaces

```
auto eth0
   iface eth0 inet static
   address 192.168.10.10
   netmask 255.255.255.0
   network 192.168.10.0
   broadcast 192.168.10.255
   gateway 192.168.10.1
```

Démarrage et arrêt du réseau

Démarrage classique

Pour un démarrage classique du service réseau, on utilise la commande /sbin/ifconfig:

- ifconfig eth0 192.168.1.12 netmask 255.255.255.0
- ifconfig eth0 up
- ifconfig eth0 down

Démarrage en utilisant les fichiers de configuration

Pour récupérer la configuration depuis les fichiers /etc/sysconfig/network et /etc/sysconfig/network-scripts, on utilise la commande /sbin/ifup

- ifup eth0



Démarrage et arrêt du réseau

Démarrage de toutes les interfaces

Pour démarrer toutes les interfaces réseaux sur un redhat on utilise la commande:

- /etc/rc.d/init.d/network start
- Cette commande récupérera des informations depuis le fichier /etc/sysctl.conf (pour le routage par exemple)

Renouvellement du bail DHCP

Pour renouveler le bail dhcp, on utilise la commande dhcpclient

Le routage

La commande route

- L'utilisation de la commande ifup permet de récupérer la passerelle depuis le fichier /etc/sysconfig/network
- À l'utilisation de la commande ifconfig (ou si la passerelle n'est pas renseignée) on pourra utiliser la commande /sbin/route pour l'ajouter à la table de routage. Par exemple:
  - route add default gw 192.168.1.1 eth0
- L'utilisation de cette commande peut s'étendre jusqu'à l'ajout de routes statiques dans la table de routage de la machine. Par exemple:
  - route add -net 192.168.1.0/24 gw 192.168.2.1 eth2

Remarque

Pour plus de commodité, on peut utiliser le nom d'un réseau au lieu de spécifier son adresse à condition que cette correspondance (nom réseau avec adresse réseau) soit indiqué dans le fichier /etc/networks

Le routage

La table de routage

```
/sbin/route -n
Table de routage IP du noyau
Destination     Passerelle    Genmask         ...  Iface
192.168.1.0     0.0.0.0       255.255.255.0   ...  eth0
192.168.2.0     0.0.0.0       255.255.255.0   ...  eth2
192.168.100.0   192.168.2.1   255.255.255.0   ...  eth2
127.0.0.0       0.0.0.0       255.0.0.0            lo
0.0.0.0         192.168.1.1   0.0.0.0              eth0
```

Remarques

- /etc/sysconfig/static-routes pour l'ajout automatique de routes statiques
- Les démons routed et gated peuvent jouer le rôle de protocoles de routage dynamique



Outils

Ping

- Cette commande envoie un paquet ICMP (echo_request) et attend sa réponse (echo_response)
- L'objectif est de vérifier si une machine sur le réseau est joignable ou non
- Options:
  - -c N : l'envoi de N paquets
  - -q : mode calme (rien n'est affiché à part le résumé)

Arp

La commande arp permet de visualiser le cache arp de la machine

```
arp
Address                  HWtype HWaddress          Flags Mask Iface
cerbere.lodyc.jussieu.f ether  00:B0:D0:D1:8B:2A  C          eth0
nestor.lodyc.jussieu.fr ether  00:04:76:E4:BB:33  C          eth0
```

Outils

Netstat

Cette commande donne des informations générales sur la configuration du réseau, à savoir:

- les tables de routage
- les statistiques des interfaces ...
- Exemple:

```
netstat -n
Connexions Internet actives (sans serveurs)
Proto  Recv-Q  Send-Q  Adresse locale      Adresse distante     Etat
tcp    0       0       134.157.9.32:22     134.157.9.52:46903   ESTABLISHED
tcp    0       0       134.157.9.32:22     134.157.9.52:46639   ESTABLISHED
tcp    0       0       134.157.9.32:800    134.157.9.11:2049    ESTABLISHED
tcp    0       0       134.157.9.32:643    134.157.9.11:111     TIME_WAIT
```

Outils

Traceroute

Cette commande affiche les différents sauts traversés pour atteindre une machine

```
traceroute to www.google.com (173.194.45.52), 30 hops max, 60 byte packets
 1  192.168.1.1  1.380 ms  2.082 ms  2.725 ms
 2  * * *
 3  81.192.65.130  73.381 ms  77.818 ms 81.192.65.138  82.380 ms
 4  81.192.65.129  84.302 ms * *
 5  193.194.50.65  98.423 ms  105.991 ms *
 6  81.192.222.8  112.312 ms  127.155 ms  130.595 ms
 7  212.217.80.18  133.653 ms  82.814 ms  85.693 ms
 8  212.217.80.9  81.247 ms  85.882 ms  75.642 ms
 9  72.14.221.166  106.529 ms  103.831 ms  152.191 ms
10  209.85.252.36  151.123 ms 209.85.252.194  164.008 ms 209.85.252.36  138.732 ms
11  216.239.43.68  147.859 ms 216.239.43.42  160.520 ms  151.011 ms
12  209.85.245.71  148.976 ms 209.85.245.82  185.738 ms  185.891 ms
13  66.249.94.79  148.433 ms  156.293 ms  151.918 ms
14  173.194.45.52  151.834 ms  145.720 ms  138.799 ms
```

Outils

Traceroute

La commande traceroute exploite le message ICMP time_exceded pour récupérer les sauts

- Elle envoie un message avec un TTL très bas
- Dès que le message d'erreur est reçu, elle incrémente le TTL et renvoie le message (pour passer au noeud suivant)